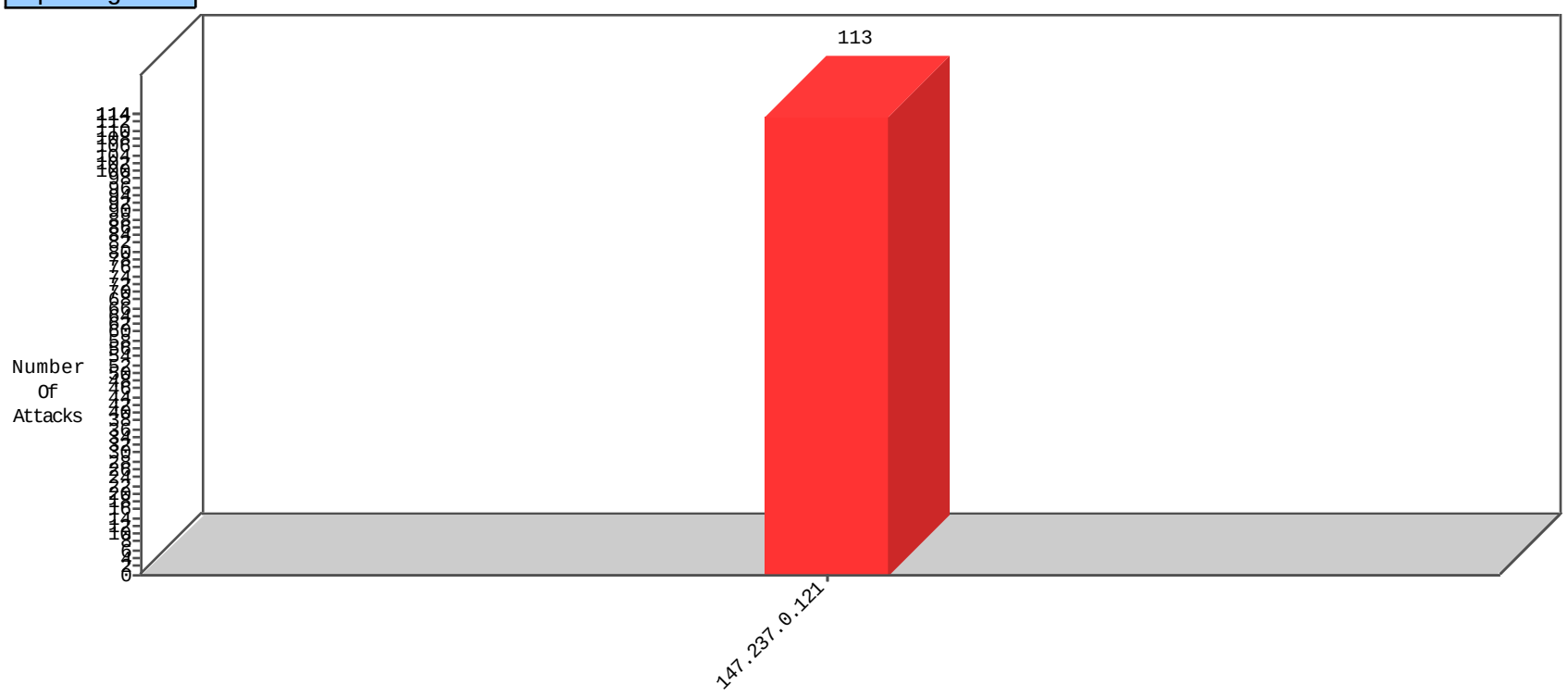
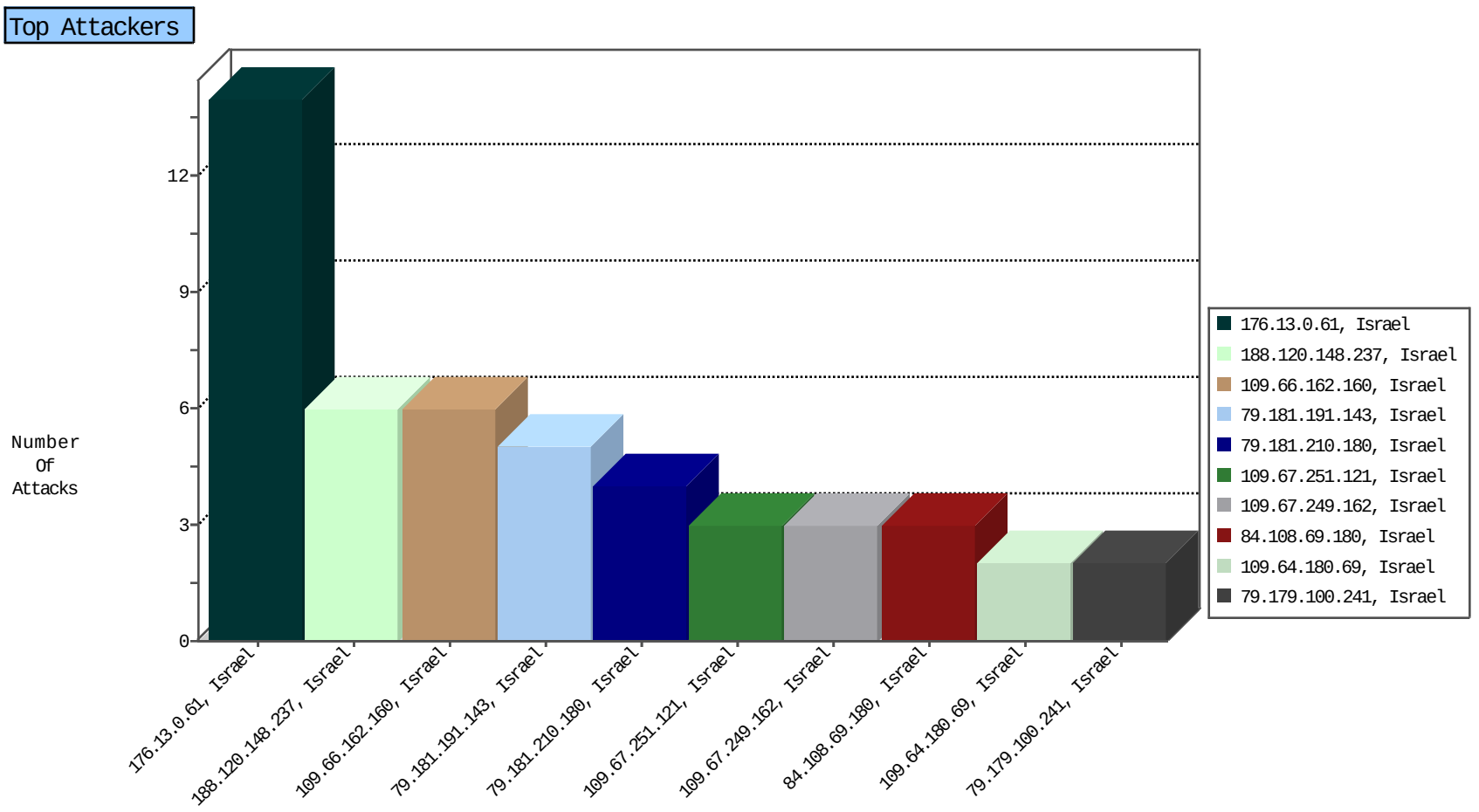
02-20-2016 to 02-21-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-20-2016 to 02-21-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
176.13.0.61	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	12

02-20-2016 to 02-21-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

02-20-2016 to 02-21-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
94.102.48.193	Netherlands	147.237.0.121		ET SCAN NMAP -sS window 1024	2
128.127.0.45	Italy	147.237.0.121		ET SCAN NMAP -sS window 1024	1
188.85.187.40	Spain	147.237.0.121		ET SCAN NMAP -sS window 1024	1
94.102.63.158	Netherlands	147.237.0.121		ET SCAN Potential SSH Scan	1
183.60.48.25	China	147.237.0.121		ET SCAN Potential SSH Scan	1

02-20-2016 to 02-21-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
149.78.242.196	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	796
149.88.142.117	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	670
149.78.146.60	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	571
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	450
80.11.121.161	France	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	416
149.78.230.177	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	411
149.88.7.127	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	315
190.195.82.13	Argentina	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	282
46.11.160.171	Malta	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	272
149.78.234.97	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	252
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	248
109.64.105.153	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	216
149.78.162.31	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	209
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	205
149.78.106.79	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	183
149.88.240.76	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	159
27.55.145.237	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	154
149.78.162.52	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	115
149.78.225.140	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	91
176.241.250.3	France	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	90
149.88.120.11	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	89
149.78.251.238	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	89
149.88.166.87	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	87
149.78.239.15	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	85
149.88.141.237	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	83
79.177.155.48	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	80
178.62.20.42	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	76
149.88.81.30	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	76
149.78.39.93	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
149.78.49.182	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
149.78.131.176	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
77.96.217.192	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
149.78.30.218	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
149.78.220.216	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
149.88.27.175	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
66.102.9.39	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
64.79.85.205	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
149.88.24.124	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
176.13.0.61	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
84.228.53.82	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.183.122.207	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
149.78.29.162	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
149.78.184.96	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
149.88.189.144	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
40.77.167.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
66.102.9.50	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.66.162.160	Israel	147.237.0.121		Suspicious Response Code	Block	6
79.181.210.180	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	4
79.181.191.143	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	3
109.67.249.162	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	3
84.108.69.180	Israel	147.237.0.121		Suspicious Response Code	Block	3
109.67.251.121	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	3
5.102.224.149	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
188.120.148.237	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
79.179.122.212	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
79.180.161.50	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
79.178.119.50	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
109.64.180.69	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
77.127.67.246	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
188.120.148.237	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.181.191.143	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
176.13.1.90	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
87.71.17.243	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
185.32.179.28	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
185.3.147.159	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
81.218.146.181	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
188.120.148.237	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 188.120.148.237 (sigalgs DoS Attack)	None	2
79.179.100.241	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	2
185.3.147.225	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
46.117.128.81	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
109.64.3.174	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
84.94.21.144	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
176.13.0.61	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.65.150.112	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.177.59.95	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
37.60.47.42	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
85.64.89.33	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
79.183.122.207	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
2.54.15.71	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
185.24.207.41	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
5.255.253.93	Russian Federation	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.179.137.74	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.65.192.91	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
79.177.125.110	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.85.225	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
80.246.136.171	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
5.29.59.84	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.181.21.5	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.181.21.5 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
79.178.233.2	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.65.29.25	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.176.80.80	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
31.210.187.138	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
84.228.53.82	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.180.15.47	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.177.243.238	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.117.67.6	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 131F91215B0B231F99A0FBFC7DA7DFA4651AADAF48CFCA300BEA0D9434E999F23DA10FBB213354550AEA5E9762135AC6043A3B457B812C5C9D79F9109D418DF10E263CF98F97954DCC8E57F5BF639637D4AFA9B1FEDB3F7528276094388031E52CF487B923B41F24ABF2422846EFBC134A3B9C4963BA852D59032DFF4AC1B960, Observed 1FE6A58E4787D6F94B0E196D0D9D170C4F686AC6D538BA38E9B829600CA68FC2F62962B2E9504F4ED70905617DE0C6064FD50ECE5706E4A31012E2A68F45F2B1FB6AC258446515AB48AB525766F37BAF9209859D7ED647DE15402861705BB93431BCAC	None	1
94.230.86.3	Israel	147.237.0.121		Suspicious Response Code	Block	1
5.29.83.198	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.21.5	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
176.13.0.61	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 176.13.0.61 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
109.65.33.27	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.177.1.72	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.46.38.19	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesIDs in www.miluim-ishi.aka.idf.il/shamapchange	Block	1
84.228.180.172	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.182.57.15	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
79.180.114.51	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.67.98.102	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.177.243.238	Israel	147.237.0.121		Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1